Recovering randomness from an asymptotic Hamming distance

Bjørn Kjos-Hanssen*

August 5, 2010

Abstract

A notion of asymptotic Hamming distance suitable for the study of algorithmic randomness is developed. As an application of this notion, it is shown that there is no fixed procedure that computes a Mises-Wald-Church stochastic set from a complex set. Here a set is complex if its prefixes have Kolmogorov complexity bounded below by an unbounded, nondecreasing computable function.

Contents

*This material is based upon work supported by the National Science Foundation under Grants No. 0652669 and 0901020.

From a distance the world looks blue and green,
and the snow-capped mountains white.

Julie Gold, 1985

1 Introduction

We are interested in the extent to which an infinite binary sequence X, or equivalently a set $X \subseteq \omega$, that is algorithmically random (Martin-Löf random) remains useful as a randomness source after modifying some of the bits of X. Usefulness here means that some algorithm (extractor) can produce a Martin-Löf random sequence from the result Y of modifying X.

If not too many bits of X are modified, the resulting set Y will have effective packing dimension 1. The question of the computational power of sets of positive effective Hausdorff dimension and packing dimension, as compared to random sets, was raised by Reimann and Terwijn around 2003 and to a great extent resolved around 2007.

Let $\leq_s$ denote Medvedev (strong) reducibility and let $\leq_w$ denote Muchnik (weak) reducibility.

Theorem 1.1 (Bienvenu, Doty, and Stephan [2])**.** *For any real numbers* $0 \leq \alpha < \beta \leq 1$*, the collection of reals* A *with* $\dim_H(A) \geq \beta$ *is not Medvedev reducible to the collection of reals with* $\dim_H(A) \geq \alpha$*.*

In particular this showed that for each Turing reduction Φ there is a set Y of positive effective Hausdorff dimension such that Φ^Y is not 1-random. By work of Greenberg and Miller this can be strengthened, making Y not depend on Φ and replacing 1-randomness by KL-stochasticity.

Theorem 1.2. *There is a set* Y *of effective Hausdorff dimension 1 such that no KL-stochastic set is Turing reducible to* Y*.*

Proof. Greenberg and Miller [8] show that there is a set Y of minimal Turing degree and effective Hausdorff dimension 1. It is easy to see that a KL-stochastic set cannot have minimal Turing degree, because if $Y = A \oplus B$ then we can use the bits in A to bet on the bits in B. □

In the present article we show that by weakening Hausdorff dimension to complex packing dimension (Definition 3.14), and weakening $\leq_w$-reducibility to $\leq_s$-reducibility, we can improve the conclusion about KL-stochasticity to MWC-stochasticity.

Definition 1.3. *An element of* 2^ω *is Mises-Wald-Church (MWC) stochastic if no partial computable monotonic selection rule can select a biased subsequence, i.e., a subsequence where the relative frequences of 0s and 1s do not converge to* $1/2$*.*

Definition 1.4. *An element of* 2^ω *is Kolmogorov-Loveland stochastic if no partial computable (non-monotonic) selection rule can select a biased subsequence, i.e., a subsequence where the relative frequences of 0s and 1s do not converge to* $1/2$.

Theorem 1.5. *There is no single Turing reduction* Φ *such that for each set* Y *of effective packing dimension 1,* Φ^Y *is MWC-stochastic.*

Actually, Theorem 1.5 arises as a corollary of a theory of *information extraction in terms of Hamming distance* that we develop an asymptotic version of herein. Information will come in two forms, randomness and diagonal non-recursiveness. A set that has small Hamming distance from a random set may be viewed as the result of an adaptive adversary corrupting or fixing some bits after looking at the original random set. Similar problems in the finite setting have been studied in computer science going back to Ben-Or and Linial [1].

Similarity and mega-standard similarity. If A is a finite set and $\sigma, \tau \in \{0,1\}^A$ then the Hamming distance $d(\sigma,\tau)$ is given by

$$d(\sigma,\tau) = |\{n : \sigma(n) \neq \tau(n)\}|\,.$$

Following Buhrman et al. [3] we write $b(n,k) := \binom{n}{0} + \cdots + \binom{n}{k}$. If a truth-table reduction Φ has disjoint uses on distinct inputs then it is natural to define, for a function $p : \omega \to \omega$,

$$X \sim_{p,\varphi} Y \quad\Longleftrightarrow\quad (\exists N)(\forall n \geq N)\ |(X+Y) \cap \varphi(n)| \leq p(n).$$

Let the collection of all infinite computable sets be denoted by $\mathfrak{C}$. Let $p : \omega \to \omega$. For $X, Y \in 2^\omega$ and $N \in \mathfrak{C}$ we write

$$X \sim_{p,N} Y \quad\Longleftrightarrow\quad (\exists n_0)(\forall n \in N,\, n \geq n_0)(d(X \upharpoonright n, Y \upharpoonright n) \leq p(n)).$$

$$X \sim_p Y \quad\Longleftrightarrow\quad X \sim_{p,\omega} Y.$$

$$X \asymp_p Y \quad\Longleftrightarrow\quad (\exists L \in \mathfrak{C})(X \sim_{p,L} Y).$$

In this paper we will develop a good understanding of $\asymp_p$ and randomness extraction. In the future one may hope to develop a similar understanding for $\sim_p$.

The relation $\asymp_p$ has a certain beauty that $\sim_p$ lacks. If X is random then, by Weber's law of the iterated logarithm for subsequences, $X \asymp_p \varnothing$ whenever $p(n) = n/2 + \omega^*(\sqrt{n})$; whereas for $\sim_p$ one has to add iterated logarithms into the picture. So $\asymp$ is the sense in which deviations do not exceed standard deviations by more than a constant amount. We can call $\asymp$ *mega-standard similarity* and say that whereas the similarity of X and $\varnothing$ is only $n/2 + (1+\varepsilon)\sqrt{2n \log\log n}$, the mega-standard similarity is lower, namely $n/2 + \omega^*(\sqrt{n})$. We can say that whereas the *asymptotic Hamming distance* between X and $\varnothing$ is bounded by $n/2 + (1+\varepsilon)\sqrt{2n\log\log n}$, the *mega-standard Hamming distance* is bounded by $n/2 + \omega^*(\sqrt{n})$.

The *mega-standard asymptotic deviation* "is $c \cdot \sqrt{n}$", i.e., it is bounded by $f(n)$ iff $f(n)$ is an unbounded nondecreasing function times the standard deviation. The *asymptotic deviation* is bounded by $(1+\varepsilon)\sqrt{2n \ln \ln n}$.

Thus if $X \asymp_p Y$ then we say that X and Y differ at most by p asymptotically, although this would be more natural if $N = \omega$.

Let us use the following notation:

$$[X]_p = \{Y : Y \asymp_p X\}.$$

Moreover,

$$[\mathcal{A}]_p = \bigcup \{[X]_p : X \in \mathcal{A}\},$$

and similarly for $[X]_{p,N}$ and $[X]_{p,\varphi}$.

2 Positive results

2.1 Extracting DNR functions

Let DNR denote the set of diagonally non-recursive functions. We consider the problem of extracting a member of DNR from a set close to a random set.

Theorem 2.1 (Michel Weber's Law of the iterated logarithm for subsequences [15])**.** *Let $\nu_1 < \nu_2 < \cdots$ be an increasing sequence of natural numbers and let $\{Y_n\}$ be an i.i.d. sequence with $\mathbb{E}(Y_n) = 0$ and $\mathbb{E}(Y_n^2) = 1$. Let $S_n = Y_1 + \cdots + Y_n$. Let*

$$p_n = \left|\{m \leq n : \{\nu_j\}_{j \geq 1} \cap (2^{m-1}, 2^m] \neq \varnothing\}\right|$$

$$\Lambda(k) = \ln p_n \quad \textit{if} \quad k \in (2^{n-1}, 2^n].$$

Then we have

$$\limsup_{j \to \infty} \frac{S_{\nu_j}}{\sqrt{2\nu_j \Lambda(\nu_j)}} = 1 \quad \textit{a.s.}$$

Remark 2.2. *In this article,* $\log$ *denotes* $\log_2$ *and* $\ln$ *denotes* $\log_e$*. Note that if $a = 2^{e^x}$ then $\ln \log a = x$, whereas*

$$\ln \ln a = \ln(e^x \ln 2) = x + \ln 2,$$

so that $\ln \log_2 \sim \ln \ln$.

The theorem, the remark, and letting $\nu_j = j$ yields the

Corollary 2.3 (Law of the iterated logarithm)**.** *Let Y_n be independent, identically distributed random variables with means zero and unit variances. Let $S_n = Y_1 + \ldots + Y_n$. Then*

$$\limsup_{n \to \infty} \frac{S_n}{\sqrt{2n \ln \ln n}} = 1$$

almost surely.

We say that $f \in \omega^\omega$ is an *order function* if f is unbounded, nondecreasing, and computable.

Theorem 2.4. *For each order function f there is a computable set $\{\nu_j\}_{j\geq 1}$ such that $\Lambda(k) \leq f(k)$ for almost all k.*

Proof. Since $\Lambda(k) = \ln p_n$ where $n = \log_2 k$, it suffices to show that $n \mapsto p_n$ can be arbitrarily slow-growing, which is clear by taking $\{\nu_j\}_{j\geq 1}$ sufficiently sparse. $\square$

Note that $|X \upharpoonright n| = d(X \upharpoonright n, \varnothing \upharpoonright n)$. For any $A \in 2^\omega$ we may consider $X + A$ given by

$$(X + A)(n) = X(n) + A(n) \mod 2.$$

Then $|(X + A) \upharpoonright n| = d(X \upharpoonright n, A \upharpoonright n)$.

Theorem 2.5. *Let X be the random variable given by $\mathbb{P}(X \in \mathcal{S}) = \lambda(\mathcal{S})$. For each A, the distribution of $X + A$ is equal to the distribution of X.*

Theorem 2.6. *If X is Kurtz random relative to A then*

$$\limsup_{n\to\infty} \frac{d(X \upharpoonright n, A \upharpoonright n) - \frac{n}{2}}{\sqrt{2n \ln\ln n}} \geq 1.$$

Proof.

$$|X \upharpoonright n| = \sum_{k<n} X_k = \frac{1}{2}\sum_{k<n}(Y_k + 1) = \frac{n}{2} + S_n$$

hence

$$\limsup_{n\to\infty} \frac{|X \upharpoonright n| - \frac{n}{2}}{\sqrt{2n \ln\ln n}} = 1$$

in particular

$$\limsup_{n\to\infty} \frac{|X \upharpoonright n| - \frac{n}{2}}{\sqrt{2n \ln\ln n}} \geq 1,$$

$$(\forall \varepsilon > 0)(\forall N)(\exists n \geq N)\left(\frac{|X \upharpoonright n| - \frac{n}{2}}{\sqrt{2n \ln\ln n}} \geq 1 - \varepsilon\right), \quad \text{and}$$

$$(\forall \varepsilon > 0)(\forall N)(\exists n \geq N)\left(|X \upharpoonright n| \geq \frac{n}{2} + (1-\varepsilon)\sqrt{2n \ln\ln n}\right).$$

almost surely. This is a Π^0_2 class of measure 1, hence each Kurtz random belongs to it. $\square$

Definition 2.7. *Let*

$$\psi_N(n) = \frac{n}{2} + \sqrt{2n\Lambda(n)},$$

$$\psi_{N,\varepsilon}(n) = \frac{n}{2} + (1-\varepsilon)\sqrt{2n\Lambda(n)},$$

Theorem 2.8. *If $X \in$ MLR and $X \sim_{\psi_{N,\varepsilon},N} A$ for some $N \in \mathfrak{C}$ then A computes a DNR function. Conversely for each $N \in \mathfrak{C}$, $X \sim_{\psi_N,N} \varnothing$ and $\varnothing$ does not compute a DNR function.*

Proof. If A does not compute a DNR function then A is Low(MLR, Kurtz) by [7]. Note that by Theorem 2.6, $\{X : X \sim_{\psi_{N,\varepsilon},N} A\}$ is $\Sigma^0_2(A)$ and of measure zero, hence contains no real that is Kurtz random in A, hence contains no ML-random real. $\square$

Definition 2.9 (Effective convergence)**.** *Let $\{a_n\}_{n\in\omega}$ be a sequence of real numbers.*

- *$\{a_n\}_{n\in\omega}$ converges to ∞ effectively if there is a computable function N such that for all k and all $n \geq N(k)$, $a_n \geq k$.*
- *$\{a_n\}_{n\in\omega}$ converges to 0 effectively if the sequence $\{a_n^{-1}\}_{n\in\omega}$ converges to ∞ effectively.*

Definition 2.10. *For a sequence of real numbers $\{a_n\}_{n\in\omega}$,*

$$\overset{*}{\lim_{n\to\infty}} a_n$$

is the real number to which a_n converges effectively, if any; and is undefined if no such number exists.

As a kind of effective big-O notation, $p = \omega^*(q)$ means $\lim^* q/p = 0$.

Theorem 2.11. *If f is any function with $f(n) = n/2 + \omega^*(\sqrt{n})$ then DNR is not Muchnik reducible to*

$$\bigcup_{N\in\mathfrak{C}} [\mathrm{MLR}]_{f,N}.$$

Proof. It suffices to show that $\varnothing \in [\mathrm{MLR}]_{f,N}$ for some $N \in \mathfrak{C}$, since clear $\varnothing$ computes no DNR function. By assumption $f(n) = n/2 + g(n)\sqrt{n}$ where $\lim^* g(n) = \infty$. By Theorem 2.1 there is a subsequence $\{\nu_j\}_{j\geq 1}$ such that for almost all X, $X \sim_{f,N} \varnothing$ where $N = \{\nu_j\}_{j\geq 1}$. $\square$

2.2 Extracting randomness

Notation. If $X \in 2^\omega$ then X is called a real, a set, or a sequence depending on context. If $I \subseteq \omega$ then $X \upharpoonright I$ denotes X, viewed as a function, restricted to the set I. We denote the cardinality of a finite set A by $|A|$. Regarding X, Y as subsets of ω and letting $+$ denote sum mod two, note that $(X + Y) \cap n = \{k < n : X(k) \neq Y(k)\}$ and generally for a set $I \subseteq \omega$, $(X + Y) \cap I = \{k \in I : X(k) \neq Y(k)\}$. If Φ is a truth-table reduction, we define the use of $\Phi^X(k)$ by

$$\varphi(k) = \{n \in \omega : (\exists Z)\ \Phi^{Z\setminus\{n\}}(k) \neq \Phi^{Z\cup\{n\}}(k)\}.$$

Majority preserves randomness. The Lebesgue measure on $[0, 1]$, or equivalently the fair-coin measure on 2^ω, is denoted by λ. For an introduction to Martin-Löf randomness the reader may consult the book by Nies [14]. Let MLR denote the set of Martin-Löf random elements of 2^ω. We use the set-theoretic notation for image,

$$R[\![A]\!] = \{y : (\exists x \in A)(\langle x, y\rangle \in R\}.$$

Lemma 2.12. *If Φ is a Turing reduction such that the random variables X and Φ^X have the same distribution, i.e, $\lambda = \lambda \circ \Phi^{-1}$, then $\Phi[\![\mathrm{MLR}]\!] \subseteq \mathrm{MLR}$.*

Proof. Let $\{U_n\}_{n\in\omega}$ be any Martin-Löf test, and let $V_n = \{X : \Phi^X \in U_n\}$. Then V_n is uniformly Σ^0_1 and $\lambda V_n = \lambda U_n$, so $\{V_n\}_{n\in\omega}$ is a Martin-Löf test. Therefore, if $X \in \mathrm{MLR}$ then $X \notin \cap_n V_n$ and hence $\Phi^X \notin \cap_n U_n$. □

Let D_k be the finite subset of ω with canonical index k, and let

$$D_k^{\mathrm{odd}} = \begin{cases} D_k & \text{if } |D_k| \text{ is an odd number or } D_k = \varnothing, \\ D_k \setminus \{\max(D_k)\} & \text{otherwise.} \end{cases}$$

Let

$$\mathrm{Maj}^X(k) = 1 \quad \Longleftrightarrow \quad \left|D_k^{\mathrm{odd}} \cap X\right| > \left|D_k^{\mathrm{odd}} \setminus X\right|.$$

This Turing reduction Maj is not itself a randomness extractor, but a simple modification will be.

Lemma 2.13. *If f is a computable function such that*

1. *$D_{f(k)} \neq \varnothing$ for each k, and*
2. *$D_{f(k)} \cap D_{f(\ell)} = \varnothing$ for all $k \neq \ell$,*

and $\Phi^X(k) = \mathrm{Maj}^X(f(k))$ for all k, then

(a) the distribution of $X \mapsto \Phi^X$ is equal to λ, and

(b) $\Phi[\![\mathrm{MLR}]\!] \subseteq \mathrm{MLR}$.

Proof. By (1), $D_{f(k)}^{\mathrm{odd}}$ is a nonempty set of odd cardinality for each k, so $\lambda\{X : \Phi^X(k) = 1\} = 1/2$ for each k. By (2), the random variables $\{\Phi^X(k)\}_{k\in\omega}$, are mutually independent. Therefore (a) follows. Part (b) follows from (a) and Lemma 2.12. □

Central Limit Theorem. Let $\mathcal{N}$ be the cumulative distribution function for a standard normal random variable; so

$$\mathcal{N}(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt.$$

Let $\mathbb{P}$ denote probability. We will make use of the following quantitative version of the central limit theorem.

Theorem 2.14 (Berry-Esséen[1]). *Let $\{X_n\}_{n\geq 1}$ be independent and identically distributed real-valued random variables with the expectations $\mathbb{E}(X_n) = 0$, $\mathbb{E}(X_n^2) = \sigma^2$, and $\mathbb{E}(|X_n|^3) = \rho < \infty$. Then there is a constant d (with $.41 \leq d \leq .71$) such that for all x and n,*

$$\left|\mathbb{P}\left(\frac{\sum_{i=1}^n X_i}{\sigma\sqrt{n}} \leq x\right) - \mathcal{N}(x)\right| \leq \frac{d\rho}{\sigma^3\sqrt{n}}.$$

[1]See for example Durrett [5], 3rd edition, page 124.

We are mostly interested in the case $X_n = X(n) \in \{0,1\}$ for $X \in 2^\omega$ under λ, in which case $\sigma = 1/2$.

Corollary 2.15. *If $g : \omega \to \omega$ with $\lim_{n\to\infty} g(n) = \infty$ and $S_n = \sum_{i=1}^n X_i$ where $\sigma = 1/2$ then*

$$\mathbb{P}(|S_n| \le g(n)) = \mathcal{O}(g(n)/\sqrt{n})$$

Proof. The Berry-Esséen Theorem 2.14 with $c := d\rho/\sigma^3$ gives that for all n,

$$\left|\mathbb{P}\left(\frac{S_n}{\sqrt{n}/2} \le x\right) - \mathcal{N}(x)\right| \le \frac{c}{\sqrt{n}}.$$

Thus using $\mathcal{N}(x) + \mathcal{N}(-x) = 1$, and the fact that for $x \ge 0$, $\mathcal{N}(x) \le \frac{1}{2} + \frac{x}{\sqrt{2\pi}}$, we have

$$\mathbb{P}(|S_n| \le x\sqrt{n}/2) = \mathbb{P}\left(\frac{S_n}{\sqrt{n}/2} \le x\right) - \mathbb{P}\left(\frac{S_n}{\sqrt{n}/2} \le -x\right)$$

$$\le \mathcal{N}(x) + \frac{c}{\sqrt{n}} - \left(\mathcal{N}(-x) - \frac{c}{\sqrt{n}}\right) = \mathcal{N}(x) - \mathcal{N}(-x) + \frac{2c}{\sqrt{n}}$$

$$= 2\mathcal{N}(x) - 1 + \frac{2c}{\sqrt{n}} \le 2\left(\frac{1}{2} + \frac{x}{\sqrt{2\pi}}\right) - 1 + \frac{2c}{\sqrt{n}} = \frac{2x}{\sqrt{2\pi}} + \frac{2c}{\sqrt{n}}$$

So if we substitute $x = 2g(n)/\sqrt{n}$,

$$\mathbb{P}\left(|S_n| \le g(n)\right) \le \frac{4g(n)}{\sqrt{2\pi n}} + \frac{2c}{\sqrt{n}} \le \text{const} \cdot \frac{g(n)}{\sqrt{n}}$$

for large enough n. □

Majority extracts randomness.

Theorem 2.16. *Suppose f and g are computable functions. For each $k \in \omega$, let $\Phi^X(k) = \mathrm{Maj}^X(f(k))$ for all $X \in 2^\omega$ and let $n_k = \left|D_{f(k)}\right|$. Suppose that the sets $\varphi(k) = D_{f(k)}$ are disjoint and nonempty. Suppose $n_{k+1} \ge n_k$ for each $k \in \omega$, and $\lim_{k\to\infty} n_k = \infty$. Suppose $g(n) = o(\sqrt{n})$ and $g(n_k)/\sqrt{n_k} \le 2^{-k}$ for all k. Then*

$$(\forall X \in \mathrm{MLR})(\forall Y \sim_{g,\varphi} X)(\Phi^Y \in \mathrm{MLR}),\ \textit{i.e.,}$$

$$\Phi[\![\mathrm{MLR}]_{g,\varphi}]\!] \subseteq \mathrm{MLR}\,.$$

Proof. Let $I_k = D_{f(k)}^{\mathrm{odd}}$ and $n_k^{\mathrm{odd}} = |I_k|$,

$$S^{(k)} = S^{(k)}[Z] = \sum_{t\in I_k}\left(Z(t) - \frac{1}{2}\right),\ \text{and note that}$$

$$\Phi^Z = \{k : S^{(k)}[Z] > 0\}.$$

Since the sets I_k are disjoint and nonempty, by Lemma 2.13 we have $\Phi[\![\mathrm{MLR}]\!] \subseteq \mathrm{MLR}$. Let

$$U_m = \left\{ Z : \left((\exists k > m) |S^{(k)}[Z]| \leq g(n_k) \right) \right\}.$$

Note that $\{U_m\}_{m\in\omega}$ is uniformly Σ^0_1.

Applying Corollary 2.15 to $n \mapsto g(n^+)$ where $n \mapsto n^+$ is the inverse of $n \mapsto n^{\mathrm{odd}}$ gives a constant C' and an N such that for all $n \geq N$,

$$\mathbb{P}\left(|S^{(k)}| \leq g(n_k) \right) \leq C' \cdot \frac{g(n_k)}{\sqrt{n_k^{\mathrm{odd}}}} \leq C \cdot \frac{g(n_k)}{\sqrt{n_k}}$$

for another constant C. Since $\lim_{k\to\infty} n_k = \infty$, there is an M such that for all $m \geq M$, $n_m \geq N$. Thus for $m \geq M$,

$$\lambda(U_m) \leq \sum_{k>m} \lambda\{Z : |S^{(k)}[Z]| \leq g(n_k)\}$$

$$\leq C \cdot \sum_{k>m} \frac{g(n_k)}{\sqrt{n_k}} \leq C \sum_{k>m} 2^{-k} = C \cdot 2^{-m}.$$

Thus $\{U_m\}_{m\in\omega}$ is a Martin-Löf test (in the extended sense). Let $X \in \mathrm{MLR}$. Then there is an m with $X \notin U_m$, hence

$$(\forall k > m)\ |S^{(k)}[X]| > g(n_k).$$

Let Y be such that $Y \sim_{g,\varphi} X$; then

$$(\forall k > m)\ \Phi^Y(k) = \Phi^X(k).$$

By Lemma 2.13, $\Phi^X \in \mathrm{MLR}$, and thus $\Phi^Y \in \mathrm{MLR}$. □

We can derive a version of Theorem 2.16 for the similarity relation $\sim_p$ as follows.

Lemma 2.17. *Let $N \in \mathfrak{C}$. If $p : \omega \to \omega$ and $g : \{n/2 : n \in \omega\} \to \omega$ are order functions with $g(n/2) = p(n)$ for all n, and Φ is a truth-table reduction whose uses $\varphi(n)$ are disjoint finite sets with $|\varphi(n)| \geq \sum_{k=0}^{n-1} |\varphi(k)|$, $\min \varphi(n+1) = \max(\varphi(n)) + 1$, and $\sum_{k=0}^{m} |\varphi(k)| \in N$ for all m, then for all X, Y, we have*

$$X \sim_{p,N} Y \quad \Longrightarrow \quad X \sim_{g,\varphi} Y.$$

Proof. Let $X \sim_p Y$ and $n_m = |\varphi(m)|$. This yields for all m,

$$|(X+Y) \cap \varphi(m)| \leq \left| (X+Y) \cap \left(\sum_{k=0}^{m} n_k \right) \right|$$

$$\leq p\left(\sum_{k=0}^{m} n_k \right) = g\left(\frac{1}{2} \sum_{k=0}^{m} n_k \right) \leq g(n_m).$$

□

Theorem 2.18. *For each order function p such that $p(n) = o(\sqrt{n})$ and each $N \in \mathfrak{C}$, there is a truth-table reduction Φ such that*

$$\Phi[\![[\mathrm{MLR}]_{p,N}]\!] \subseteq \mathrm{MLR}\,.$$

Proof. Let $g : \{n/2 : n \in \omega\} \to \omega$ be an order function such that $g(n/2) = p(n)$ for all n. Note that $\frac{g(n)}{\sqrt{n}} = \sqrt{2} \cdot \frac{p(2n)}{\sqrt{2n}} \to 0$.

Define $h : \omega \to \mathbb{R}$ by

$$h(n) = \frac{\sqrt{n}}{g(n)},$$

so $\lim_n h(n) = \infty$. We may assume $\lim_n g(n) = \infty$, since otherwise we may take Φ to be the identity map $\Phi^Z = Z$. Thus we can let $k \mapsto n_k$ be a sufficiently fast-growing computable sequence to guarantee that

$$\frac{1}{h(n_k)} \leq 2^{-k}, \quad n_m \geq \sum_{k=1}^{m-1} n_k,$$

and $\sum_{k=0}^{m} n_k \in N$ for all m. Let $I_k = D_{f(k)}$ be disjoint finite sets of size n_k such that $\min I_{k+1} = \max I_k + 1$. For each $k \in \omega$, let $\Phi^X(k) = \mathrm{Maj}^X(f(k))$ for all $X \in 2^\omega$. By Lemma 2.17, if $X \sim_{p,N} Y$ then $X \sim_{g,\varphi} Y$. By Theorem 2.16 we are done. □

3 Negative results

3.1 The Hamming cube

The Hamming distance between a point and a set of points is defined by $d(y, A) := \min_{a\in A} d(y, a)$. The d-neighborhood of a set $A \subseteq \{0,1\}^n$ is

$$\Gamma_d(A) = \{y \in \{0,1\}^n : d(y, A) \leq d\}.$$

In particular,

$$\Gamma_d(\{c\}) = \{y \in \{0,1\}^n : d(y, c) \leq d\},$$

and

$$\Gamma_d(A) = \bigcup_{a\in A} \Gamma_d(\{a\}).$$

A *Hamming-sphere*[2] with center $c \in \{0,1\}^n$ is a set $S \subseteq \{0,1\}^n$ such that for some k,

$$\Gamma_k(\{c\}) \subseteq S \subseteq \Gamma_{k+1}(\{c\}).$$

Theorem 3.1 (Harper [9]; see also Frankl and Füredi [6])**.** *For each $n \geq 1$ and each set $A \subseteq \{0,1\}^n$, there is a Hamming-sphere $S \subseteq \{0,1\}^n$ such that*

$$|A| = |S|\,, \quad \textit{and}$$

$$|\Gamma_d(A)| \geq |\Gamma_d(S)|\,.$$

[2] A Hamming-sphere is more like a ball than a sphere, but the terminology is entrenched.

Note that for all $c \in \{0,1\}^n$, $|\Gamma_k(\{c\})| = b(n,k)$. We define

$$B_r^I(\sigma) = \Gamma_d(\{\sigma\}) = \{\tau \in \{0,1\}^I : d(\sigma,\tau) \le r\}.$$

Unless otherwise indicated, the probability $\mathbb{P}$ of a set $E \subseteq \{0,1\}^I$ is by definition

$$\mathbb{P}(E) = \frac{|E|}{2^{|I|}},$$

i.e., $\mathbb{P}$ is counting measure scaled to be a probability measure.

Lemma 3.2 (Key Lemma)**.** *Let $☹ \in \omega^\omega$. Suppose*

$$\overset{*}{\lim_{n\to\infty}} ☹(n)/\sqrt{n} = \infty. \tag{1}$$

Let $f \in \omega^\omega$ be a computable function. Let $I_m = D_{f(m)}$[3] and $n_m = |I_m|$. Suppose

$$\overset{*}{\lim_{m\to\infty}} n_m = \infty. \tag{2}$$

For each $m \in \omega$ let $E_m \subseteq \{0,1\}^{I_m}$. Suppose $\limsup_{m\to\infty} \mathbb{P}(E_m) \le \mathfrak{p}$ *where $0 < \mathfrak{p} < 1$ is computable. Writing*

$$\mathbb{P}(B_{☹(n)}(X) \subseteq E_m) := \mathbb{P}(B^{I_m}_{☹(n_m)}(X \upharpoonright I_m) \subseteq E_m),$$

we have

$$\overset{*}{\lim_{m\to\infty}} \mathbb{P}(B_{☹(n)}(X) \subseteq E_m) = 0. \tag{3}$$

Moreover, for each $m_0 \in \omega$ and computable $\mathfrak{q} \in (\mathfrak{p}, 1)$ there is a modulus of effective convergence in (3) that works for all sets $\{E_m\}_{m\in\omega}$ such that for all $m \ge m_0$, $\mathbb{P}(E_m) \le \mathfrak{q}$.

Proof. Let $p_m = \mathbb{P}(E_m)$. Let $r = r_m$ be such that

$$b(n,r) \le |E_m| < b(n, r+1).$$

Let

$$q_t = b(n,t) \cdot 2^{-n}.$$

Then

$$q_r \le p_m < q_{r+1}.$$

Let us write

$$B_t(X) := B_t^{I_m}(X \upharpoonright I_m),$$

considering $X \upharpoonright I_m$ as a string of length n. By Harper's Theorem 3.1, we have a Hamming sphere H with $|H| = |\neg E_m|$ and

$$\left|\Gamma_{☹(n)}(\neg E_m)\right| \ge \left|\Gamma_{☹(n)}(H)\right|, \quad \text{i.e.,}$$

[3]Recall that D_m is the m^{th} canonical finite set, and note that we do not assume the sets I_m are disjoint.

$$\mathbb{P}(\{X : X \in \Gamma_{\frownie(n)}(\neg E_m)\}) \geq \mathbb{P}(\{X : X \in \Gamma_{\frownie(n)}(H)\}).$$

Therefore

$$\mathbb{P}(\{X : X \notin \Gamma_{\frownie(n)}(\neg E_m)\}) \leq \mathbb{P}(\{X : X \notin \Gamma_{\frownie(n)}H)\}).$$

Let $\widehat{H}$ be the complement of H. Then

$$\mathbb{P}(\{X : B_{\frownie(n)}(X) \subseteq E_m\}) \leq \mathbb{P}(\{X : B_{\frownie(n)}(X) \subseteq \widehat{H}\}).$$

If the Hamming sphere H is centered at $c \in \{0,1\}^n$ then clearly the complement $\widehat{H}$ is a Hamming sphere centered at $\overline{c}$, where $\overline{c}(k) = 1 - c(k)$. Since $p_m 2^n = |E_m|$, $\left|\widehat{H}\right| = |E_m|$, and $p_m \leq q_{r+1} = b(n, r+1)2^{-n}$, we have $\widehat{H} \subseteq \Gamma_{b(n,r+1)}(\{\overline{c}\})$, so

$$\begin{aligned}\mathbb{P}(B_{\frownie(n)}(X) \subseteq \widehat{H}) &\leq \mathbb{P}(B_{\frownie(n)}(X) \subseteq \Gamma_{b(n,r+1)}(\{\overline{c}\})) \\ &= \frac{b(n, r+1-\frownie(n))}{2^n} = q_{r+1-\frownie(n)}.\end{aligned}$$

If we let $X \in 2^\omega$ be a random variable whose distribution is λ, then we can define the further random variable

$$S^{(m)} = \sum_{i \in I_m} X(i)$$

and note that

$$q_{r+1-\frownie(n)} = \mathbb{P}[S^{(m)} \leq r + 1 - \frownie(n)]$$

Let $Y_i = X_i - \mathbb{E}(X_i)$ where $\mathbb{E}(X_i) = \frac{1}{2}$ is the expected value of X_i, so $\mathbb{E}(Y_i) = 0$. By the Berry-Esséen Theorem 2.14, for all x

$$\left|\mathbb{P}\left(\frac{\sum_{i \in I_m} Y_i}{\sigma\sqrt{n}} \leq x\right) - \mathcal{N}(x)\right| \leq \frac{d\rho}{\sigma^3\sqrt{n}} = \frac{d}{\sqrt{n}},$$

where $\rho = 1/8 = \mathbb{E}(|Y_i|^3)$, and $\sigma = 1/2$ is the standard deviation of X_i (and Y_i). Thus if we let

$$f_m(x) = \mathbb{P}\left(\frac{S^{(m)} - n/2}{\sqrt{n}/2} \leq x\right)$$

then

$$|f_m(x) - \mathcal{N}(x)| \leq \frac{d}{\sqrt{n_m}}$$

Since $\lim^*_m n_m = \infty$, $\lim^* \frac{d}{\sqrt{n_m}} = 0$. So

$$\lim_{m \to \infty}^{*} \sup_x |f_m(x) - \mathcal{N}(x)| = 0. \tag{4}$$

Let

$$a_m = \frac{r_m - \frac{n}{2}}{\sqrt{n}/2} \quad \text{and} \quad b_m = a_m + \frac{1}{\sqrt{n}/2} - \frac{\frownie(n)}{\sqrt{n}/2}.$$

Then

$$\mathbb{P}[S^{(m)} \leq r+1-☹(n)] = \mathbb{P}\left[\frac{S^{(m)}-\frac{n}{2}}{\sqrt{n}/2} \leq \frac{r+1-\frac{n}{2}-☹(n)}{\sqrt{n}/2}\right]$$

$$= f_m\left(a_m + \frac{1}{\sqrt{n}/2} - \frac{☹(n)}{\sqrt{n}/2}\right) = f_m(b_m).$$

By (4),

$$\overset{*}{\lim_{m\to\infty}} |f_m(b_m) - \mathcal{N}(b_m)| = 0. \tag{5}$$

We have

$$\limsup_{m\to\infty} f_m(a_m) = \limsup_{m\to\infty} \mathbb{P}\left(\frac{S^{(m)}-n/2}{\sqrt{n}/2} \leq \frac{r_m-\frac{n}{2}}{\sqrt{n}/2}\right)$$

$$= \limsup_{m\to\infty} \mathbb{P}(S^{(m)} \leq r_m) = \limsup_{m\to\infty} q_{r_m} \leq \limsup_{m\to\infty} p_m \leq \mathfrak{p}$$

Since $f_m \to \mathcal{N}$ uniformly, it follows that

$$\limsup_{m\to\infty} \mathcal{N}(a_m) \leq \mathfrak{p}.$$

and so as $\mathcal{N}$ is strictly increasing,

$$\limsup_{m\to\infty} a_m \leq \mathcal{N}^{-1}(\mathfrak{p}) \quad (= 0 \text{ if } \mathfrak{p} = 1/2).$$

Since

$$\overset{*}{\lim_{m\to\infty}} \frac{1}{\sqrt{n}/2} = 0,$$

and by assumption $\lim^*_n ☹(n)/\sqrt{n} = \infty$, we have that b_m is the sum of a term that goes effectively to 0, a term that goes effectively to $-\infty$, and a term whose $\limsup$ is at most $\mathcal{N}^{-1}(\mathfrak{p})$, so that after a fixed term it never goes above say $\mathcal{N}^{-1}(\mathfrak{p})+1$ again. Thus

$$\overset{*}{\lim} b_m = -\infty,$$

and so

$$\overset{*}{\lim} \mathcal{N}(b_m) = 0.$$

Hence by (5), $\lim^* f_m(b_m) = 0$. Since we showed that $\lim^* f_m(b_m) = 0$, and since by assumption $\lim^* n_m = \infty$,

$$\overset{*}{\lim_{m\to\infty}} \mathbb{P}(B_{☹(n)}(X) \subseteq E_m) = 0.$$

□

3.2 Stochastically dominated sets

Let μ_1 and μ_2 be probability measures on sample spaces Ω_1 and Ω_2 and let E be a measurable subset of $\Omega_1 \times \Omega_2$. The projections of E are $E^x = \{y : (x, y) \in E\}$ and $E_y = \{x : (x, y) \in E\}$.

We may write

$$\mathbb{P}(\text{Event}) = \lambda\{X : X \in \text{ Event}\}.$$

Theorem 3.3. *Suppose that η, α, and δ are positive real numbers such that*

$$\mu_1 E_y > \eta \quad (\forall y \in \Omega_2), \quad \textit{and} \tag{6}$$

$$\mu_1\{x : \mu_2 E^x \leq \alpha\} \geq 1 - \delta. \tag{7}$$

Then $\eta < \alpha + \delta$.

Proof. By Fubini's theorem,

$$\eta < \int_{\Omega_2} \mu_1(E_y) d\mu_2(y) = \iint\limits_{\Omega_1 \times \Omega_2} E(x, y) d\mu_1(x) d\mu_2(y) = \int_{\Omega_1} \mu_2(E^x) d\mu_1(x)$$

$$\leq \alpha \cdot \mu_1\{x : \mu_2(E^x) \leq \alpha\} + 1 \cdot \mu_1\{x : \mu_2(E^x) \geq \alpha\} \leq \alpha \cdot 1 + 1 \cdot \delta.$$

□

Definition 3.4. *A set X is immune if for each $N \in \mathfrak{C}$, $N \not\subseteq X$. If $\omega \setminus X$ is immune then X is co-immune. If X is both immune and co-immune then X is bi-immune.*

Definition 3.5. *A set X is stochastically bi-immune if for each set $N \in \mathfrak{C}$, $X \upharpoonright N$ satisfies the strong law of large numbers, i.e.,*

$$\lim_{n\to\infty} \frac{|X \cap N \cap n|}{|N \cap n|} = \frac{1}{2}.$$

Definition 3.6. *Let $0 \leq \mathfrak{p} < 1$. A sequence $X \in 2^\omega$ is* $\mathfrak{p}$-stochastically dominated *if for each $L \in \mathfrak{C}$,*

$$\limsup_{n\to\infty} \frac{|L \cap n|}{n} > 0 \quad \Longrightarrow \quad (\exists M \in \mathfrak{C}) \quad M \subseteq L \quad \textit{and} \quad \limsup_{n\to\infty} \frac{|X \cap M \cap n|}{|M \cap n|} \leq \mathfrak{p}.$$

The class of stochastically dominated sequences is denoted $\mathrm{SD} = \mathrm{SD}_{\mathfrak{p}}$*. If $\omega \setminus X \in$* $\mathrm{SD}_{\mathfrak{p}}$ *then we write $X \in \mathrm{SD}^{\mathfrak{p}}$ and say that X is stochastically dominating.*

It is clear that each MWC-stochastic set is $\frac{1}{2}$-stochastically dominated and clearly each finite set is in $\mathrm{SD}_{\mathfrak{p}}$ for each $\mathfrak{p}$.

Definition 3.7. *For a real X and a string σ of length n,*

$$(\sigma \searrow X)(n) = \begin{cases} \sigma(n) & \textit{if } n < |\sigma|, \\ X(n) & \textit{otherwise.} \end{cases}$$

$$(\sigma^\frown X)(n) = \begin{cases} \sigma(n) & \text{if } n < |\sigma|, \\ X(n - |\sigma|) & \text{otherwise.} \end{cases}$$

Thinking of σ and X as functions we may write

$$\sigma \searrow X = \sigma \cup (X \upharpoonright \omega \backslash |\sigma|)$$

and thinking in terms of concatenation we may write

$$\sigma^\frown X = \sigma\, X$$

Lemma 3.8. *Let Φ be a Turing reduction such that*

$$\lambda(\Phi^{-1}[\![\mathrm{SD}_{\mathfrak{p}}]\!]) = 1 \tag{8}$$

and let $\Phi^X_\sigma = \Phi^{\sigma \searrow X}$. Then for any finite set $\Sigma \subseteq 2^{<\omega}$, a subsequence of the random variables $\{\Phi^X_\sigma(i)\}_{i\in\omega}$ converges to a distribution stochastically dominated[4] *by the $\mathfrak{p}$-coin distribution uniformly over $\sigma \in \Sigma$, i.e.,*

$$(\forall \Sigma)(\forall \varepsilon > 0)(\forall i_0)(\exists i > i_0)(\forall \sigma \in \Sigma)$$
$$\mathbb{P}(\{X \mid \Phi^X_\sigma(i) = 1\}) \le \mathfrak{p} + \varepsilon.$$

Proof. First note that for all $\sigma \in 2^{<\omega}$, $\lambda(\Phi^{-1}_\sigma[\![\mathrm{SD}_{\mathfrak{p}}]\!] = 1$ as well.

Suppose otherwise, and fix ε, i_0 and Σ such that

$$(\forall i > i_0)(\exists \sigma \in \Sigma) \quad \mathbb{P}(\Phi^X_\sigma(i) = 1) > \mathfrak{p} + \varepsilon.$$

By density of the rationals in the reals we may assume ε is rational and hence computable. Since there are infinitely many i but only finitely many σ, it follows that there is some σ such that

$$(\exists^\infty k > i_0) \quad \mathbb{P}(\Phi^X_\sigma(k) = 1) > \mathfrak{p} + \varepsilon \tag{9}$$

and in fact

$$\limsup \left|\{k < n : \mathbb{P}(\Phi^X_\sigma(k) = 1) > \mathfrak{p} + \varepsilon\}\right| / n > 0.$$

Fix such a σ and let $\Psi = \Phi_\sigma$. Let $\{\ell_n\}_{n\in\omega}$ be infinitely many values of k in (9) listed in increasing order; note that $\mathcal{L} = \{\ell_n\}_{n\in\omega}$ may be chosen as a computable sequence.

For an as yet unspecified subsequence $\mathcal{K} = \{k_n\}_{n\in\omega}$, $\mathcal{K} \subseteq \mathcal{L}$, let

$$E = \{(X, n) : \Psi^X(k_n) = 1\}. \tag{10}$$

We obtain then also projections $E_n = \{X : \Psi^X(k_n) = 1\}$, $E^X = \{n : \Psi^X(k_n) = 1\}$. By (9) we have for all $n \in \omega$,

$$\lambda E_n > \mathfrak{p} + \varepsilon. \tag{11}$$

[4] In a different sense from $\mathrm{SD}_{\mathfrak{p}}$.

The fraction of events E_n that occur in $N = \{0, \ldots, N-1\}$ for X is denoted

$$e_{N,X} = \frac{|E^X \cap N|}{N}$$

By assumption (8),

$$\lambda\left\{X : (\exists \mathcal{K} \subseteq \mathcal{L})(\exists M)(\forall N \geq M)\left(e_{N,X} \leq \mathfrak{p} + \frac{\varepsilon}{2}\right)\right\} = 1.$$

Thus there is an M and a $\mathcal{K}$ (using that $\mathfrak{C}$ is countable) such that

$$\lambda\left\{X : e_{M,X} \leq \mathfrak{p} + \frac{\varepsilon}{2}\right\} \geq \lambda\left\{X : (\forall N \geq M)e_{N,X} \leq \mathfrak{p} + \frac{\varepsilon}{2}\right\} \geq 1 - \frac{\varepsilon}{3}. \qquad (12)$$

Let Ω_1 be the unit interval $[0,1]$. Let $\Omega_2 = M = \{0, 1, \ldots, M-1\}$. Let $\mu_1 = \lambda$. Let $\mu_2 = \text{card}$ be the counting measure on the finite set $M = \{0, 1, \ldots, M-1\}$, so that for a finite set $A \subset M$, $\text{card}(A)$ is the cardinality of A. [5] Let $\eta = \mathfrak{p} + \varepsilon$, $\alpha = \mathfrak{p} + \varepsilon/2$, and $\delta = \varepsilon/3$, and note that $\eta > \alpha + \delta$. By (11), (12) and Theorem 3.3, $\eta < \alpha + \delta$, a contradiction. $\square$

Let the *use* $\varphi^X(n)$ be the largest number used in the computation of $\Phi^X(n)$. (This is slightly different from our earlier definition of use.) We write

$$\Phi^X(n) \downarrow @s$$

if $\Phi^X(n)$ halts by stage s, with use at most s; if this statement is false, we write $\Phi^X(n) \uparrow @s$. We may assume that the running time of a Turing reduction is the same as the use, because any X-computable upper bound on the use is a reasonable notion of use.

Let IM denote the set of immune sets (i.e., sets that are infinite but contain no infinite computable sets), CIM the set of co-immune sets (i.e., sets whose complements are immune), $\text{SD}^{\mathfrak{p}}$ the set of complements of sets in SD_p, and W3R the set of weakly 3-random sets.

Theorem 3.9. *Let $p : \omega \to \omega$ be any computable function such that $p(n) = \omega^*(\sqrt{n})$. Let Φ be a Turing reduction. There exists an $N \in \mathfrak{C}$ and an almost sure event $\mathcal{A}$ such that for all $X \in \mathcal{A}$, there is a set $Y \sim_{p,N} X$ such that $\Phi^Y \notin \mathcal{A}$, i.e.,*

$$(\forall X \in \mathcal{A}) \quad \Phi[\![[X]_p]\!] \not\subseteq \mathcal{A}.$$

More specifically, let $\mathcal{A} = \text{W3R}$ and

$$\mathcal{B} = (\text{SD}_{\mathfrak{p}} \cap \text{CIM}) \cup (\text{SD}^{\mathfrak{p}} \cap \text{IM}).$$

Then $\lambda\mathcal{A} = \lambda\mathcal{B} = 1$ and

$$(\forall X \in \mathcal{A})(\exists Y \sim_p X)(\Phi^Y \notin \mathcal{B}).$$

[5] In this case, $\int \mu_1(E_y) d\mu_2(y) = \int \mu_1(E_n) d\mu_2(n) = \int \lambda(E_n) d\,\text{card}(n) = \sum_{n \in \Omega_2} \lambda(E_n)\,\text{card}(\{n\}) = \sum_{n=0}^{M-1} \lambda(E_n) \cdot 1$.

Proof. Let $\mathcal{S} = \{X \mid \exists Y \sim_p X\ \Phi^Y \notin \text{MLR}\}$. Let $\mathfrak{p} < 1$ be computable. We show

1. If $\lambda(\Phi^{-1}[\![\text{SD}_\mathfrak{p}]\!]) = 1$, or $\lambda(\Phi^{-1}[\![\text{SD}^\mathfrak{p}]\!]) = 1$, then
$$\text{MLR} \subseteq \{X : (\exists Y \sim_p X)\ \Phi^Y \notin \text{CIM}\} \subseteq \mathcal{S}, \quad \text{or}$$
$$\text{MLR} \subseteq \{X : (\exists Y \sim_p X)\ \Phi^Y \notin \text{IM}\} \subseteq \mathcal{S}, \quad \text{respectively.}$$
2. Otherwise; then
$$\text{W3R} \subseteq \{X : (\exists Y =^* X)\ \Phi^Y \notin \text{SD}_\mathfrak{p} \text{ and } (\exists Y =^* X)\ \Phi^Y \notin \text{SD}^\mathfrak{p}\} \subseteq \mathcal{S}.$$

Proof of (2): If we are not in case (1) then $\lambda\{X \mid \Phi^X \in \text{SD}_\mathfrak{p}\} < 1$, so by the 0-1 Law, $\lambda\{X \mid (\forall Y =^* X)(\Phi^Y \in \text{SD}_\mathfrak{p})\} = 0$. This is (contained in) a Π^0_3 null class, so if $X \in \text{W3R}$ then $(\exists Y =^* X)(\Phi^Y \notin \text{SD}_\mathfrak{p})$ hence since $\text{MLR} \subseteq \text{SD}_\mathfrak{p}$, $X \in \mathcal{S}$. So we are done.
Proof of (1): By Lemma 3.8,

$$(\exists \mathfrak{p} < 1)(\forall \varepsilon > 0)(\forall n)(\forall i)(\exists i' > i)(\forall \sigma \in 2^{=n})$$

$$\mathbb{P}(\{Z : \Phi^{\sigma \searrow Z}(i') = 1\}) \leq \mathfrak{p} + \varepsilon; \tag{13}$$

Since Φ is total for almost all oracles, it is clear that i' is a computable function $f(k, n)$ of $\varepsilon = 1/k$ and n. Let $g : \omega \to \omega$ be the computable function with $\lim_{n\to\infty} g(n) = \infty$ given by $g(s) = 2s$. Let $n_0 = 0$ and $i_0 = 0$. Assuming $s \geq 0$ and n_s and i_s have been defined, let

$$i_{s+1} = f(g(s), n_s),$$

and let n_{s+1} be a stage at which Φ has converged a great deal, i.e., so large that

$$(\forall \sigma \in 2^{=n_s}) \quad \lambda\{Z \mid \Phi^{\sigma \searrow Z}(i_{s+1}) \uparrow @n_{s+1}\} \leq \frac{1}{2s}, \tag{14}$$

and such that n_{s+1} is large enough that

$$\frac{p(n_{s+1} - n_s)}{\sqrt{n_{s+1} - n_s}} \to^* \infty \quad \text{and} \quad \sum_{k=0}^{s} p(n_{k+1} - n_k) \leq p(n_{s+1}).$$

This completes the definition on the function $s \mapsto (n_s, i_s)$. Note that since $i' > i$ in 13, we have $i_{s+1} > i_s$ and hence $R := \{i_0, i_1, \ldots\}$ is a computable infinite set. We now have

$$(\forall s)(\forall \sigma \in 2^{=n_s}) \quad \mathbb{P}(\{Z : \Phi^{\sigma \searrow Z}(i_{s+1}) = 1\}) \leq \mathfrak{p} + \frac{1}{2s} \tag{15}$$

so

$$\mathbb{P}(\{Z : \Phi^{\sigma \searrow Z}(i_{s+1}) \downarrow = 1 @ n_{s+1}\}) \leq \mathfrak{p} + \frac{1}{2s}. \tag{16}$$

Note $[a, b) = b \backslash a$.

Let $X \in \mathrm{MLR}$. We aim to define $Y \sim_p X$ such that $\Phi^Y \notin \mathrm{MLR}$. We will in fact make $Y \leq_T X$, so we define a reduction Ξ and let $Y = \Xi^X$. Since we are defining Y by modifying bits of X, the use of Ξ will be the identity function: $\xi^X(n) = n$.

Recall that $n_0 = 0$. Thus we have no choice but to declare that $Y \upharpoonright n_0$ equals the empty string. So suppose $s \geq 0$ and $Y_{\upharpoonright n_s}$ has already been defined. The set of "good" strings now is

$$\mathcal{G} = \{\tau \succ Y_{\upharpoonright n_s} \mid \Phi^{\tau \upharpoonright n_{s+1}}(i_{s+1}) = 0\}.$$

Define the "cost" of τ to be the additional Hamming distance to X, i.e., $d(\tau) = |(X + \tau) \cap [n_s, n_{s+1})|$.

Case 1. $\mathcal{G} \neq \varnothing$. Then let $Y_{\upharpoonright n_{s+1}}$ be any $\tau_0 \in \mathcal{G}$ of length n_{s+1} and of minimal cost, i.e., such that $d(\tau_0) = \min\{d(\tau) \mid \tau \in \mathcal{G}\}$.

Case 2. Otherwise. Then make no further changes to X up to length n_{s+1}, i.e., let $Y_{\upharpoonright n_{s+1}} = Y_{\upharpoonright n_s} \searrow X_{\upharpoonright n_{s+1}}$.

This completes the definition of Ξ and hence of Y. It remains to show that $\Phi^Y \notin \mathrm{MLR}$. Let

$$\begin{aligned} E_{s+1} &= \left\{Z : \neg \left(\Phi^{\sigma \searrow Z}(i_{s+1}) \downarrow = 0 @ n_{s+1}\right), \text{ where } \sigma := \Xi^X \upharpoonright n_s\right\}. \\ &= \left\{Z : \left(\Phi^{\sigma \searrow Z}(i_{s+1}) \downarrow = 1 @ n_{s+1}\right), \text{ where } \sigma := \Xi^X \upharpoonright n_s\right\} \\ &\quad \cup \left\{Z : \left(\Phi^{\sigma \searrow Z}(i_{s+1}) \uparrow @ n_{s+1}\right), \text{ where } \sigma := \Xi^X \upharpoonright n_s\right\} \end{aligned}$$

Since (14) and (16) hold for all strings of length n_s, in particular they hold for $\sigma = \Xi^X \upharpoonright n_s$, so

$$(\forall s) \quad \mathbb{P}(E_{s+1}) \leq \mathfrak{p} + \frac{1}{2s} + \frac{1}{2s} = \mathfrak{p} + \frac{1}{s}, \quad \text{hence} \quad \lim_{s \to \infty} \mathbb{P}(E_{s+1}) = \mathfrak{p}. \tag{17}$$

Let

$$U_s^{X \upharpoonright n_s} = \{Z : B_{p(n_{s+1} - n_s)}(Z) \subseteq E_{s+1}\}.$$

One may say that the oracle for E_{s+1} is $X \upharpoonright n_s$, and the Hamming cube for E_{s+1} is $\{0,1\}^{[n_s, n_{s+1})} \ni X \upharpoonright [n_s, n_{s+1})$.

By Lemma 3.2, $\mathbb{P}(U_s^{X \upharpoonright n_s}) \to 0$ effectively, for all $X \in 2^\omega$, using

$$\frac{p(n_{s+1} - n_s)}{\sqrt{n_{s+1} - n_s}} \to^* \infty.$$

Also by Lemma 3.2 there is an effective modulus of convergence $h(s)$ that only depends on an upper bound for an s_0 such that for all $s \geq s_0$, $\mathbb{P}(E_{s+1}) \leq \mathfrak{q}$ (where $\mathfrak{p} < \mathfrak{q} < 1$ and $\mathfrak{q}$ is just some fixed computable number). Since by (17) such an upper bound can be given that works for all X, actually $h(s)$ may be chosen to not depend on X. Finally, a diagonalization: let

$$V_s = \{Z : Z \in U_s^{Z \upharpoonright n_s}\},$$

then V_s is uniformly Σ^0_1. To find the probability of V_s we use the law of iterated expectations: for two random variables A and B on the same probability space, $\mathbb{E}(A) = \mathbb{E}(\mathbb{E}(A \mid B)) = \mathbb{E}_b[\mathbb{E}(A \mid B = b)]$. We get

$$\mathbb{P}(V_s) = \mathbb{E}(\mathbf{1}_{V_s}) = \mathbb{E}(\mathbb{E}(\mathbf{1}_{V_s} \mid Z \upharpoonright n_s))$$

$$= \mathbb{E}_\sigma[\mathbb{E}(\mathbf{1}_{V_s} \mid Z_{\upharpoonright n_s} = \sigma)] = \mathbb{E}_\sigma[\mathbb{E}(\mathbf{1}_{U^\sigma_s} \mid Z_{\upharpoonright n_s} = \sigma)] = \mathbb{E}_\sigma[\mathbb{E}(\mathbf{1}_{U^{Z\upharpoonright n_s}_s} \mid Z_{\upharpoonright n_s} = \sigma)]$$

$$= \mathbb{E}(\mathbb{E}(\mathbf{1}_{U^{Z\upharpoonright n_s}_s} \mid Z \upharpoonright n_s)) \leq \mathbb{E}(h(s)) = h(s)$$

so since $\lim^*_{s\to\infty} h(s) = 0$, $\{V_s\}_{s\in\omega}$ is a Martin-Löf test. Let $\{m_s\}_{s\in\omega}$ be a computable sequence such that $\sum_{s\geq t} h(m_s) \leq 2^{-t}$. Let $W_t = \bigcup_{s\geq t} V_{m_s}$. Then $\mathbb{P}(W_t) \leq 2^{-t}$ and W_t is uniformly Σ^0_1. Since $X \in \mathrm{MLR}$, $X \notin W_t$ for some t and hence $X \notin V_{m_s}$ for all but finitely many s. So $\Phi^Y(m_s) = 0$ for all but finitely many s, hence $\Phi^Y \notin \mathrm{CIM}$. By construction, we have

$$|(X + Y) \cap [n_s, n_{s+1})| \leq p(n_{s+1} - n_s)$$

for all but finitely many n. Therefore

$$|(X + Y) \cap [0, n_{s+1})| \leq \sum_{k=0}^{s} p(n_{k+1} - n_k) \leq p(n_{s+1})$$

so $X \sim_{p,N} Y$ where $N = \{n_s : s \in \omega\}$. □

3.3 Complex versus MWC-stochastic sequences

There are three notions of *stochastically dominating immune* (SDI).

Definition 3.10. *Assume A is immune.*

1. *A is SDI if for each $N \in \mathfrak{C}$, $\liminf_{n\in N} \geq \mathfrak{p}$.*
2. *A is densely SDI if for each $N \in \mathfrak{C}$, there is $M \in \mathfrak{C}$, $M \subseteq N$, with $\liminf_{n\in M} \geq \mathfrak{p}$.*
3. *A is weakly SDI (SDI$^-$) if for each $N \in \mathfrak{C}$ of positive upper density, there is $M \in \mathfrak{C}$, $M \subseteq N$, with $\liminf_{n\in M} \geq \mathfrak{p}$.*

Note that $\mathrm{SDI}^- = \mathrm{SD}^{1/2} \cap \mathrm{IM}$.

Theorem 3.11. *If $A \in \mathrm{SDI}$ then A is not computably traceable.*

Proof. We trace the function $f(n) = A \upharpoonright I_n \in D_{h(n)}$ where I_n are large (size ℓ) disjoint intervals and $D_{h(n)} = \{\sigma_0, \sigma_1, \ldots\}$ is of size $p(n)$. Let i_0 be the majority value of σ_0 and let $B_0 = \{k : \sigma_0(k) = i\}$. Let i_{s+1} be the majority value of $\sigma_s \upharpoonright B_s$ and let $B_{s+1} = \{k : \sigma_{s+1}(k) = i_{s+1}\} \cap B_s$. The cardinality of $B_{p(n)}$ is at least $\ell \cdot 2^{-p(n)}$ and $A \upharpoonright B_{p(n)}$ is a constant a_n. Let ℓ_n be much larger than ℓ_t, $t < n$.

If for infinitely many n, $a_n = 0$ then there is $N \in \mathfrak{C}$ on which A is not dominating, so A is not in SDI. Otherwise, all but finitely many $a_n = 1$, and so A is not immune. □

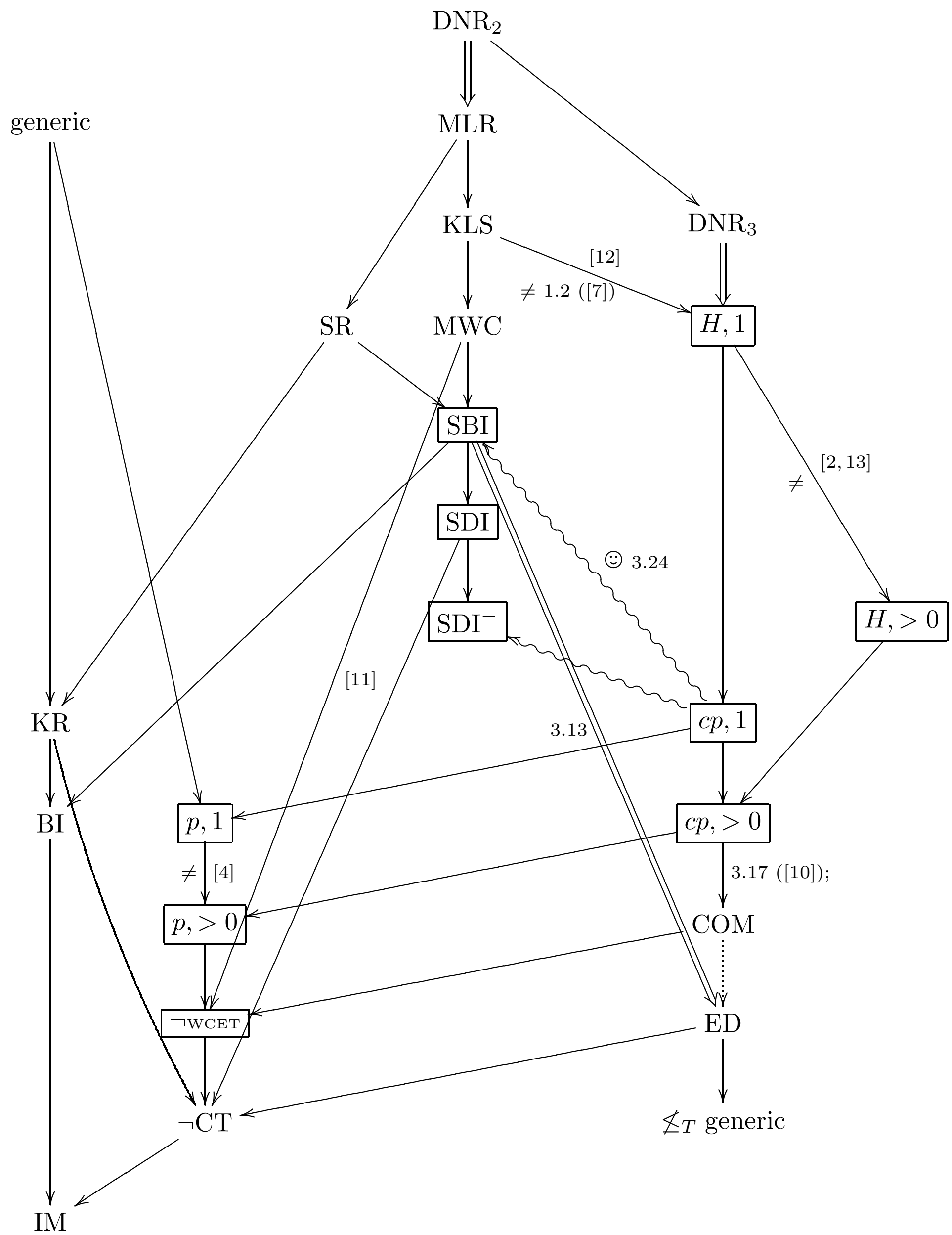

Figure 1: Some Medvedev degrees. See Figures 2 and 3 for definitions.

$\dashrightarrow$ Muchnik above

$\longrightarrow$ Included in

$\rightsquigarrow$ Not Medvedev above

$\Longrightarrow$ Medvedev above

Figure 2: Meaning of arrows.

Abbreviation	Unabbreviation	Definition
DNR	Diagonally non-recursive function in ω^ω	
DNR_n	Diagonally non-recursive function in n^ω	
MLR	Martin-Löf random	
KLR	Kolmogorov-Loveland random (MLR$\equiv_s$KLR)	
SR	Schnorr random	
KR	Kurtz random (weakly 1-random)	
MWC	Mises-Wald-Church stochastic	1.3
KLS	Kolmogorov-Loveland stochastic	1.4
SBI	Stochastically bi-immune	3.5
BI	bi-immune	3.4
IM	immune (equivalently under $\equiv_s$: noncomputable)	3.4
$(H, 1)$	effective Hausdorff dimension 1	3.14
$(H, > 0)$	effective Hausdorff dimension > 0	3.14
$(p, 1)$	effective packing dimension 1	3.14
$(p, > 0)$	effective packing dimension > 0	3.14
$(cp, 1)$	complex packing dimension 1	3.14
$(cp, > 0)$	complex packing dimension > 0	3.14
COM	complex in the sense of [10]	3.16
ED	eventually different	3.12
$\not\leq_T$ Cohen generic	not computable from a 2-generic set	
CT	computably traceable	
WCET	weakly c.e. traceable	3.18

Figure 3: Abbreviations used in Figure 1.

Definition 3.12. *A function $f \in \omega^\omega$ is* eventually different *(ED) if for each computable function $g \in \omega^\omega$, $\{x : f(x) = g(x)\}$ is finite.*

Theorem 3.13. SBI $\geq_s$ ED.

Proof. Let $A \in$ SBI and suppose the function $f(n) = A \upharpoonright I_n$ is equal to a computable function $g(n)$ for each $n \in C$, where $C \in \mathfrak{C}$.

Here I_n are large (size ℓ) disjoint intervals. Let ℓ_n be much larger than ℓ_t, $t < n$.

Consider the set M of majority positions on the strings $g(n)$, $n \in C$.

Either infinitely often the majority is 0, or infinitely often it is 1. Either way M witnesses that $A \notin$ SBI. $\square$

Definition 3.14. *The* effective Hausdorff dimension *of $A \in 2^\omega$ is*

$$\liminf_{n\in\omega} \frac{K(A \upharpoonright n)}{n}.$$

The complex packing dimension *of $A \in 2^\omega$ is*

$$\dim_{cp}(A) = \sup_{N\in\mathfrak{C}} \inf_{n\in N} \frac{K(A \upharpoonright n)}{n}.$$

The effective packing dimension *of $A \in 2^\omega$ is*

$$\limsup_{n\in\omega} \frac{K(A \upharpoonright n)}{n}.$$

Theorem 3.15. *For all $A \in 2^\omega$,*

$$0 \leq \dim_H(A) \leq \dim_{cp}(A) \leq \dim_p(A) \leq 1.$$

Proof. The inequality $\dim_H(A) \leq \dim_{cp}(A)$ uses the fact that each cofinite set $N \subseteq \omega$ is in $\mathfrak{C}$. The inequality $\dim_{cp}(A) \leq \dim_p(A)$ uses the fact that each $N \in \mathfrak{C}$ is an infinite subset of ω. $\square$

Definition 3.16 ([10])**.** *$A \in 2^\omega$ is* complex *if there is an order function h with $K(A \upharpoonright n) \geq h(n)$ for almost all n.*

The terminology *complex packing dimension* is due to the following theorem. There is similarly a natural notion of *autocomplex packing dimension* $\dim_{ap}$, obtained by requiring the set N to be recursive in A, with the property that $\dim_{ap}(A) > 0$ implies that A is autocomplex [10], but we will not study it here.

Theorem 3.17. *If $\dim_{cp}(A) > 0$ then A is complex.*

Proof. Suppose $\dim_{cp}(A) > 0$. Then there is an $N \in \mathfrak{C}$ and an $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$ such that $\inf_{n\in N} K(A \upharpoonright n)/n \geq \varepsilon$. Thus for all $n \in N$, $K(A \upharpoonright n) \geq \varepsilon n$. Let $N = \{n_0 < n_1 < \cdots\}$, let $m_t = \lceil n_t/\varepsilon \rceil$, and let $f(t) = A \upharpoonright m_t$. Then $K(f(t)) \geq t$ and $f \leq_{wtt} A$. Now [10, Theorem 2.6(4)-(6)] implies that A is complex, once we notice that the proof given there works equally well for prefix complexity as for plain complexity. $\square$

Definition 3.18 (Nies [14])**.** *$A \in 2^\omega$ is* facile *if $K(A \upharpoonright n \mid n) \le h(n)$ for all order functions h and almost all n. If A is not facile then A is* difficult*. A is weakly c.e. traceable if for each order function p, for all computably bounded functions $f \le_T A$, there is a c.e. trace for f of size bounded by p.*

Theorem 3.19 (Nies [14])**.** *A is weakly c.e. traceable iff $\forall Z \le_T A$, Z is facile.*

Theorem 3.20. *A complex set cannot be weakly c.e. traceable.*

Proof. Suppose $K(A \upharpoonright n) \ge h(n)$ where h is an order function. Applying an inverse to h we get $K(A \upharpoonright g(n)) \ge n$ for an order function g. Then $A \upharpoonright g(n)$ is computably bounded, and cannot be traced by a very small trace, or else it would have complexity $O(\log n)$. $\square$

Theorem 3.21 (Merkle [11])**.** *If A is MWC-stochastic then $K(A \upharpoonright n) \neq O(\log n)$.*

Corollary 3.22. *If A is MWC-stochastic then A is difficult.*

Lemma 3.23. *Suppose $f(n) = \frac{\delta n + o(n)}{\log n}$. If $X \in \mathrm{MLR}$ and $X \asymp_f Y$ then $\dim_{cp}(Y) \ge 1 - \delta$.*

Proof. Suppose there are at most $f(n)$ many bits changed to go from the random real X to the real Y, in positions $a_1, \ldots, a_{f(n)}$. (In cases there are fewer than $f(n)$ changed bits, we can repeat a_i representing the bit 0 which we may assume is changed.) Let $(Y \upharpoonright n)^*$ be a shortest description of $Y \upharpoonright n$. From the code

$$0^{|K(Y \upharpoonright n)|} {}^\frown 1 {}^\frown K(Y \upharpoonright n) {}^\frown (Y \upharpoonright n)^* {}^\frown a_1 \cdots a_{f(n)}$$

we can effectively recover $X \upharpoonright n$. Thus

$$n - c_1 \le K(X \upharpoonright n) \le 2\log[K(Y \upharpoonright n)] + 1 + K(Y \upharpoonright n) + f(n)\log n + c_2$$

$$\le 2\log[n + 2\log n + c_3] + 1 + K(Y \upharpoonright n) + f(n)\log n + c_2.$$

Hence

$$n \le^+ 3\log n + K(Y \upharpoonright n) + f(n)\log n, \quad \text{and}$$

$$n - (f(n) + 3)\log n \le^+ K(Y \upharpoonright n).$$

Thus $\dim_p(Y) \ge \delta + \varepsilon$ for each $\varepsilon > 0$. $\square$

Since the numbers n_{s+1} are computable, the reals we obtain have effective packing dimension 1 in an especially effective way.

Theorem 3.24. *For each Turing reduction procedure Φ there is a set Y with $\dim_{cp}(Y) = 1$ such that Φ^Y is not MWC-stochastic.*

Proof. Let $p(n) = n^{2/3}$, so that $p(n) = o(n/\log n)$ and $p(n) = \omega^*(\sqrt{n})$. By Theorem 3.9, for each weakly 3-random set X there is a set $Y \sim_p X$ such that Φ^Y is not both co-immune and in $\mathrm{SD}_{1/2}$, in particular Φ^Y is not MWC-stochastic. By Lemma 3.23, each such Y has constructive dimension 1. $\square$

We can argue that it is not surprising that Theorem 3.24 holds: A 1-generic set G satisfies $\dim_p(G) = 1$, but does not compute an ED function. An MWC-stochastic set uniformly computes an ED function. Thus, were Theorem 3.24 to fail, the mere knowledge that a computable set N exists witnessing $\dim_{cp}(Y) = 1$, without knowing an index for N, would somehow allow to compute an ED function. Our results do not rule out the possibility that for each $N \in \mathfrak{C}$ and $c \in \omega$ and f there is a Φ which produces an MWC-stochastic set from any set Y with $K(Y \upharpoonright n) \geq n - (f(n)+3)\log n - c$ for all $n \in N$, and Theorem 3.24 should not be taken as evidence that the analogous result for Mučnik reducibility holds.

It seems potentially more surprising that one cannot uniformly get a SDI$^-$ set from a set with $\dim_{cp} = 1$, since in this case we do not yet know whether a 1-generic set computes such a set.

References

[1] M. Ben-Or and N. Linial, *Collective coin flipping*, Randomness and Computation (S. Micali, ed.), Academic Press, New York, 1989, 1989, pp. 91-115. ↑3

[2] Laurent Bienvenu, David Doty, and Frank Stephan, *Constructive dimension and Turing degrees*, Theory Comput. Syst. **45** (2009), no. 4, 740–755, DOI 10.1007/s00224-009-9170-1. MR2529744 ↑2, 20

[3] Harry Buhrman, Lance Fortnow, Ilan Newman, and Nikolai Vereshchagin, *Increasing Kolmogorov complexity*, STACS 2005, Lecture Notes in Comput. Sci., vol. 3404, Springer, Berlin, 2005, pp. 412–421. MR2151636 (2006c:68091) ↑3

[4] Chris J. Conidis, *A real of strictly positive effective packing dimension that does not compute a real of effective packing dimension one*, Submitted. ↑20

[5] Richard Durrett, *Probability: theory and examples*, 2nd ed., Duxbury Press, Belmont, CA, 1996. MR1609153 (98m:60001) ↑7

[6] P. Frankl and Z. Füredi, *A short proof for a theorem of Harper about Hamming-spheres*, Discrete Math. **34** (1981), no. 3, 311–313, DOI 10.1016/0012-365X(81)90009-1. MR613409 (83a:05004) ↑10

[7] Noam Greenberg and Joseph S. Miller, *Lowness for Kurtz randomness*, J. Symbolic Logic **74** (2009), no. 2, 665–678. MR2518817 (2010b:03050) ↑6, 20

[8] ———, *Diagonally non-recursive functions and effective Hausdorff dimension*, Bulletin of the London Mathematical Society, to appear. ↑2

[9] L. H. Harper, *Optimal numberings and isoperimetric problems on graphs*, J. Combinatorial Theory **1** (1966), 385–393. MR0200192 (34 #91) ↑10

[10] Bjørn Kjos-Hanssen, Wolfgang Merkle, and Frank Stephan, *Kolmogorov complexity and the recursion theorem*, Transactions of the American Mathematical Society (January 28, 2010), in press. ↑20, 21, 22

[11] Wolfgang Merkle, *The complexity of stochastic sequences*, J. Comput. System Sci. **74** (2008), no. 3, 350–357, DOI 10.1016/j.jcss.2007.06.018. MR2384080 (2009e:68051) ↑20, 23

[12] Wolfgang Merkle, Joseph S. Miller, André Nies, Jan Reimann, and Frank Stephan, *Kolmogorov-Loveland randomness and stochasticity*, Ann. Pure Appl. Logic **138** (2006), no. 1-3, 183–210, DOI 10.1016/j.apal.2005.06.011. MR2183813 (2006h:68074) ↑20

[13] Joseph S. Miller, *Extracting information is hard: a Turing degree of non-integral effective Hausdorff dimension*, Advances in Mathematics, to appear. ↑20

[14] André Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009. MR2548883 ↑6, 23

[15] Michel Weber, *The law of the iterated logarithm on subsequences—characterizations*, Nagoya Math. J. **118** (1990), 65–97. MR1060703 (92a:60089) ↑4